Amendments to the Claims

Please amend Claims 1 and 20. The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

1. (Currently amended) In a computer network, apparatus for mapping data between different security domains, the apparatus comprising:

a communication module stored on a computer-readable medium for establishing a communication connection between a sender of one security domain and a receiver in a different security domain, wherein the communication connection is a secure communication channel formed by the communication module (i) authenticating the sender with the communication module and authenticating the receiver with the communication module, resulting in an authorized sender and authorized receiver, and (ii) encrypting working data transmitted over the channel;

a mapping module stored on a computer-readable medium coupled to the communication module for anonymously mapping working data of the one security domain to working data of the different security domain, the working data having (i) a research data portion and (ii) a personal identifier portion related to identifying a person associated with the research data portion, the mapping module mapping the personal identifier portion of the working data in the one security domain to the personal identifier portion of the working data in the different security domain such that the working data transmitted to the receiver over the secure communication channel is anonymous data, while leaving the research data portion unmapped by the anonymous mapping of the personal identifier portions; and

a secret sharing module stored on a computer-readable medium for performing secret sharing to control keyholder access to the mapping module such that a predetermined number of keyholders greater than one is required to compromise access to the mapping module;

the apparatus communicating between parties comprising at least the sender and the receiver in at least two different security domains;

wherein the communication module is capable of (i) transmitting both the anonymously mapped personal identifier portion and the unmapped research data portion of the working data to the receiver over the secure communication channel, and (ii) transmitting from the receiver to the sender a return of the working data based on a reverse mapping performed by the mapping module;

and wherein the anonymous mapping of the personal identifier portion is a one-to-one mapping.

2. (Original) Apparatus as claimed in Claim 1 wherein the research data portion of the working data includes personal data of individuals.

3. (Canceled)

4. (Previously presented) Apparatus as claimed in Claim 1 wherein the mapping module employs encryption in the mapping of the personal identifier portion of the working data in the one security domain to the personal identifier portion of the working data in the different security domain such that the working data transmitted to the authorized receiver is anonymous data.

5. (Canceled)

6. (Canceled)

7. (Previously presented) Apparatus as claimed in Claim 1 further comprising permanent storage means for storing data in a tamper-proof manner.

8. (Original) Apparatus as claimed in Claim 7 wherein the permanent storage means encrypts non-queried parts of the data, said encryption using an encryption key, and the secret sharing module storing the encryption key.

9. (Original) Apparatus as claimed in Claim 8 wherein the permanent storage means employs digital signatures on queried parts of the data to detect changes in data and thereby prevent tampering.

10. (Original) Apparatus as claimed in Claim 9 wherein each digital signature is formed from a message digest of a concatenation of the encryption key and data.

11. (Original) Apparatus as claimed in Claim 9 wherein the permanent storage means maintains a summary measure of stored data.

12. (Original) Apparatus as claimed in Claim 11 wherein said summary measure has a respective digital signature.

13. (Previously presented) Apparatus as claimed in Claim 1 wherein the mapping module defines a mapping between any two security domains by storing a mapping table having cross references between personal identifier portions of working data of the two security domains.

14. (Previously presented) Apparatus as claimed in Claim 13 wherein the mapping module stores a mapping table for plural security domains, the mapping table being formed of (i) an index section and (ii) a working reference section, the index section indicating a personal identifier portion of working data in a first security domain and the working reference section indicating a corresponding personal identifier portion in a second security domain, the working reference being encrypted, such that the mapping module performs decryption on a part of the mapping table to determine a usable cross reference of the working data.

15. (Previously presented) Apparatus as claimed in Claim 1 wherein the mapping module maps working data among plural security domains.

16. (Original) Apparatus as claimed in Claim 1 wherein the sender and receiver are respectively one of a software implementation and a human being.

17. (Original) Apparatus as claimed in Claim 1 wherein connection of the sender and receiver is in respective different sessions.

18. (Original) Apparatus as claimed in Claim 1 wherein the communication module further enables communication connection by a supervisor in addition to the sender and receiver.

19. (Original) Apparatus as claimed in Claim 18 wherein the communication connection by the supervisor enables remote operation of the apparatus by the supervisor.

20. (Currently amended) A method for transferring and mapping data between different security domains in a computer network, comprising the steps of:

using a communication module stored in a computer-readable medium, establishing a communication connection between a sender in one security domain and a receiver in a different security domain, wherein the communication connection is a secure communication channel formed by the communication module (i) authenticating the sender with the communication module and authenticating the receiver with the communication module, resulting in an authorized sender and authorized receiver, and (ii) encrypting working data transmitted over the channel;

using the communication module, transmitting working data from the authorized sender to the authorized receiver, the working data having (i) a research data portion and (ii) a personal identifier portion related to identifying a person associated with the research data portion;

using a mapping module stored in a computer-readable medium, anonymously mapping the working data of the one security domain to working data of the different security domain by mapping between the personal identifier portion of the working data in the one security domain and the personal identifier portion of the working data in the different security domain, the mapping between the personal identifier portions being performed such that the working data received by the receiver over the secure communication channel is anonymous data, while leaving the research data portion unmapped by the anonymous mapping of the personal identifier portions;

using a secret-sharing module stored in a computer-readable medium,

controlling keyholder access to the mapping using secret sharing such that a predetermined number of keyholders greater than one is required to compromise access to the mapping module;

wherein transmitting the working data using the communication module comprises transmitting both the anonymously mapped personal identifier portion and the unmapped research data portion of the working data to the receiver over the secure communication channel;

wherein the communication module is capable of transmitting from the receiver to the sender a return of the working data based on a reverse mapping performed by the mapping module; and

wherein the anonymous mapping of the personal identifier portion is a one-to-one mapping.

21. (Original) A method as claimed in Claim 20 wherein the step of transmitting includes including personal data of individuals in the research data portion.

22. (Canceled)

23. (Previously presented) A method as claimed in Claim 20 wherein the step of mapping the personal identifier portions includes encrypting such that the working data received by the authorized receiver is anonymous data.

24. (Canceled)

25. (Original) A method as claimed in Claim 20 further comprising the step of storing data in a tamper-proof manner in a permanent storage.

26. (Original) A method as claimed in Claim 25 wherein the step of storing includes encrypting non-queried parts of the data.

27. (Original) A method as claimed in Claim 26 wherein the step of storing further includes assigning a respective digital signature to each queried part of the data to enable detection of changes in the data and thereby prevent tampering.

28. (Original) A method as claimed in Claim 27 wherein the step of encrypting employs an encryption key, and the step of assigning includes forming a digital signature from a message digest of a concatenation of data and the encryption key.

29. (Original) A method as claimed in Claim 27 wherein the step of storing working data includes maintaining a summary measure of stored data.

30. (Original) A method as claimed in Claim 29 wherein the step of maintaining a summary measure includes assigning a digital signature to the summary measure.

31. (Previously presented) A method as claimed in Claim 20 wherein the step of mapping includes storing a mapping table having cross references between the personal identifier portions of the working data of the two security domains.

32. (Previously presented) A method as claimed in Claim 31 wherein the step of storing a mapping table includes storing a respective mapping table for each security domain, each mapping table being formed of (i) an index section and (ii) a working reference section, the index section indicating a personal identifier portion of working data in a first security domain and the working reference section indicating a corresponding personal identifier portion in a second security domain, the working reference being encrypted; and decrypting a part of the mapping table to determine a usable cross reference of the working data.

33. (Previously presented) A method as claimed in Claim 20 wherein the step of mapping includes mapping working data among plural security domains.

34. (Original) A method as claimed in Claim 20 wherein the sender and receiver are respectively one of a software implementation and a human being.

35. (Previously presented) A method as claimed in Claim 20 wherein the step of establishing a communication connection between the sender and receiver includes connecting the sender in one session and connecting the receiver in a different session.

36. (Original) A method as claimed in Claim 20 further comprising the step of connecting a supervisor to the computer network.

37. (Original) A method as claimed in Claim 36 further comprising the step of enabling remote control by the supervisor.

38. (Previously presented) Apparatus as claimed in Claim 1 wherein the personal identifier portion of the working data includes personal identifiers from plural security domains, the mapping module mapping multiple personal identifiers between multiple security domains for each research portion of the working data.

39. (Original) Apparatus as claimed in Claim 1 further comprising:

a secured container;

a computer system executing the communication module and the mapping module; and

a firewall coupled to the computer system, the computer system and firewall being housed by the secured container so as to provide tamper-proof hardware.

40. (Previously presented) An apparatus according to claim 1, wherein the working data is formed of plural records, each record comprising (i) a research data portion and (ii) a personal identifier portion related to identifying an individual person associated with the research data portion, the individual person being the same person across each record of the plural records.

41. (Previously presented) A method according to claim 20, wherein the working data is formed of plural records, each record comprising (i) a research data portion and (ii) a personal identifier portion related to identifying an individual person associated with the research data portion, the individual person being the same person across each record of the plural records.